National Aeronautics and Space Administration

Internal Control Program Handbook

July 24, 2008

Table of Contents

Section 1: Use of the Internal Control Program Handbook

1.1 Introduction

This Internal Control Program (ICP) handbook explains the approach that NASA uses to implement requirements pursuant to Section 2 of the Federal Managers' Financial Integrity Act (FMFIA) and its implementing guidance by the Office of Management and Budget (OMB), Circular A-123, Management's Responsibility for Internal Control. The FMFIA requires the Administrator to submit to the President, Congress, and OMB an annual statement on whether there is reasonable assurance that the Agency's internal controls are achieving their intended objectives, as well as a report on material weaknesses in NASA controls. In general, such controls are intended to ensure the effectiveness, efficiency, and safety of Agency operations; safeguard NASA assets from unauthorized use or disposition; and ensure compliance with applicable laws and standards. The FMFIA also calls for the Government Accountability Office (GAO) to establish general internal control standards for use across government.

The NASA implementation of FMFIA uses results from an annual request for Statement of Assurance (SoA) certifications submitted by all Officials-in-Charge (OICs) and Center Directors who are direct reports to the Administrator. Certification results provide evidence to support the Administrator's signed SoA reported outside the Agency. Section 1.2 provides the objectives of this handbook. Section 1.3 provides the external regulatory framework, and Section 1.4 describes the GAO standards for internal control. Section 1.5 explains NASA's internal control governance structure of responsibilities assigned to the Administrator and extending through specific organizations and down to every employee. Section 2 of the ICP handbook presents an annual operating structure of internal control activities that flow through planning to follow-up on identifying and correcting deficiencies and then planning for the next cycle of SoA internal control assessments. Section 3 of the handbook provides a standard set of evaluation tools for performing the SoA assessment.

Implementing an effective NASA control structure and process to mitigate the many risks that NASA faces is important for successful accomplishment of mission and mission support activities. In implementing the ICP, the Agency is better positioned to reach the goals and requirements set forth in the NASA Strategic Management and Governance Handbook, the NASA Strategic Plan, and all NASA policies and procedures. The ICP builds on NPD 1200.1, which vests overall responsibility for administering the program with the Assistant Administrator for Internal Controls and Management Systems. The program emphasizes the importance of an internal control structure with work processes strengthened by policy implementation that fosters more dynamic and integrated roles for programmatic, institutional, and financial organizations.

1.2 Objectives

Primary objectives of this ICP handbook are to:

- Present the governance structure for NASA internal control including a description of roles and responsibilities;
- Describe the methodology of the SoA process from new fiscal year planning through end-of-year publication of the Administrator’s SoA, and a lessons learned follow-up in planning for the next year’s activity;
- Present a standard list of work activities to be reviewed against the 5 GAO standards
- Provide a standard survey to be used in certifying internal control;
- Provide the template for transmitting the Statement of Assurance certification.

The ICP handbook will be reviewed annually by the Senior Assessment Team (SAT) to ensure that it adequately reflects the structure and requirements of NASA’s SoA process for internal control. The SAT serves as an arm of the Operations Management Council (OMC) to ensure appropriate risk identification and corrective action tracking, manage updates to the ICP, and oversee the analysis of internal control certifications. The data call for Statements of Certification will include an annually updated ICP handbook on requirements and processes that contribute to the Administrator’s Statement of Assurance.

1.3 Framework

NASA is subject to numerous legislative and regulatory requirements that promote and support effective internal control. Recent government-wide initiatives have been implemented to improve program management, as well as financial management, including tracking corrective actions for material weaknesses in internal control related to financial reporting, imposing accelerated reporting due dates for more timely financial information, and assessing the effectiveness and efficiency of program operations using the Program Assessment Rating Tool (PART). Activities conducted as part of these initiatives support NASA’s overall internal control framework. Statutory requirements that should also be considered as part of NASA’s internal control framework include:

Federal Managers Financial Integrity Act of 1982 (FMFIA) (31 U.S.C. 3512 (b) and (c) Federal Managers’ Financial Integrity Act (P.L. 97-255), 96 Stat. 814, September 8, 1982.)
The FMFIA requires agencies to establish and maintain internal control. The agency head must annually evaluate and report on the control and financial systems that protect the integrity of Federal programs; Section 2 and Section 4 respectively.

Government Performance and Results Act of 1993 (GPRA) (31 U.S.C. §1115 note)
To support results-oriented management, GPRA requires agencies to develop strategic plans, set performance goals, and report annually on actual performance compared to goals. With the implementation of this legislation, these plans and goals are integrated into (i) the budget process, (ii) the operational management of agencies and programs, and (iii) accountability reporting to the public on performance results, and on the integrity, efficiency, and effectiveness with which they are achieved. Similarly, the PART’s primary purpose is to assess program effectiveness and improve program

performance. The PART has also become an integral part of the budget process when making funding resource allocations or decisions.

Chief Financial Officers Act of 1990, as amended (CFO Act)
The CFO Act requires agencies to both establish and assess internal control related to financial reporting. The Act requires the preparation and audit of financial statements. In this process, auditors report on internal control and compliance with laws and regulations related to financial reporting. Therefore, the agencies covered by the Act have a clear opportunity to improve internal control over their financial activities, and to evaluate the controls that are in place.

Inspector General Act of 1978, as amended (IG Act) (5 U.S.C. App., et seq.)
The IG Act provides for independent reviews of agency programs and operations. IGs are required to submit semiannual reports to Congress on significant abuses and deficiencies identified during the reviews and the recommended actions to correct those deficiencies. IGs and/or external auditors are required by the Government Auditing Standards and OMB Bulletin No. 07-04, Audit Requirements of Federal Financial Statements to report material weaknesses in internal control related to financial reporting and noncompliance with laws and regulations as part of the financial statement audit. Auditors also provide recommendations for correcting the material weaknesses. Agency managers, who are required by the IG Act to follow up on audit recommendations, should use these reviews to identify and correct problems resulting from inadequate or poorly designed controls, and to build appropriate controls into new programs. Audit work planned by the IG should be coordinated with management’s assessment requirements to ensure cost effectiveness and avoid duplication.

Federal Financial Management Improvement Act of 1996 (FFMIA) (P.L. 104- 208)
The FFMIA requires agencies to have financial management systems that substantially comply with the Federal financial management systems requirements, standards promulgated by the Federal Accounting Standards Advisory Board (FASAB), and the U.S. Standard General Ledger (USSGL) at the transaction level. Financial management systems shall have general and application controls in place in order to support management decisions by providing timely and reliable data. The agency head makes a determination annually about whether the agency’s financial management systems substantially comply with the FFMIA. If the systems are found not to be compliant, management develops a remediation plan to bring those systems into substantial compliance. Management must determine whether non-compliances with FFMIA should also be reported as non-conformances with Section 4 of FMFIA.

Federal Information Security Management Act of 2002 (FISMA) (44 U.S.C. 3541 et seq.)
The FISMA provides, “…a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets…” Agencies are required to provide information security controls proportionate with the risk and potential harm of not having those controls in place. Agency heads are required to annually report on the effectiveness of the agencies’ security programs. “Significant deficiencies” found under FISMA must also be reported as material weaknesses under FMFIA.

Improper Payments Information Act of 2002 (IPIA) (P.L. 107-330)
The IPIA requires agencies to review and, “…identify programs and activities that may be susceptible to significant improper payments.” Agencies must annually submit estimates of improper payments, corrective actions to reduce the improper payments, and statements as to whether its current information

systems and infrastructure can support the effort to reduce improper payments. The nature and incidence of improper payments shall be considered when assessing the effectiveness of internal control.

Clinger-Cohen Act of 1996 (40 U.S.C. 1401, et seq., section 808 of Public Law 104-208) [formerly known as the Information Technology Management Reform Act, Division E of Public Law 104-106.] The Clinger-Cohen Act requires agencies to use a disciplined capital planning and investment control (CPIC) process to maximize the value of and assess and manage the risks of the information technology acquisitions.

1.4 Standards

Internal control includes the plan of organization, methods and procedures adopted by management to meet its goals. Internal control includes processes for planning, organizing, directing, controlling, and reporting on agency operations.

The three objectives of internal control are:

- Effectiveness and efficiency of operations,
- Reliability of financial reporting, and
- Compliance with applicable laws and regulations.

The safeguarding of assets is a subset of all of these objectives. Internal control should be designed to provide reasonable assurance regarding prevention of or prompt detection of unauthorized acquisition, use or disposition of assets.

Management is responsible for developing and maintaining internal control activities that comply with the following standards to meet the above objectives:

- Control Environment,
- Risk Assessment,
- Control Activities,
- Information and Communications, and
- Monitoring

A. Control Environment

Management and employees should establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward internal control and conscientious management.

B. Risk Assessment

Internal control should provide for an assessment of the risks the Agency faces from both external and internal sources.

C. Control Activities

Internal control activities help ensure that management's directives are carried out. The control activities should be effective and efficient in accomplishing the agency's control objectives.

D. Information and Communications

Information should be recorded and communicated to management and others within the entity who need it and in a form and within a time frame that enables them to carry out their internal control and other responsibilities.

E. Monitoring

Internal control monitoring should assess the quality of performance over time and ensure that the findings of audits and other reviews are promptly resolved.

1.5 Governance Structure

1.51 The NASA Administrator

By law, every head of each government entity is the senior official who provides an annual Statement of Assurance on the status of internal control within the organization. The NASA Administrator is responsible for the following:

- Serve as the highest authority for reasonable assurance of internal control throughout the Agency;
- Certify and sign the annual Statement of Assurance on the status of internal control published in NASA’s ***Annual Financial Report*** submitted to OMB, the Congress, and the President, pursuant to the Federal Managers’ Financial Integrity Act and the Government Performance and Results Act.

1.5.2 The NASA Deputy Administrator

The Deputy Administrator is the Administrator’s lead official for monitoring internal control. Responsibilities are to:

- Advise the Administrator of the contents of each year’s Statement of Assurance;
- Chair the OMC meetings on internal control;
- Oversee internal control planning and decision-making by the OMC;
- Decide on recommendations to add a major deficiency to the OMC Watch List; change the significance level of an existing deficiency; and approve actions to close a deficiency;
- Act as the primary decision-maker on what deficiencies must be reported annually as material weaknesses;
- If unavailable for an OMC meeting, delegate chairmanship to the Associate Administrator.

1.5.3 The Operations Management Council

The OMC, chaired by the Deputy Administrator, is NASA's senior council for oversight of corrections to major deficiencies maintained on the Council's Watch List. The OMC consists of NASA OICs, Center Directors, and the Inspector General (ex officio). The OMC's authority derives from the NASA Strategic Management and Governance Handbook. Responsibilities of members are to:

- Provide oversight of internal control within their organization and more broadly across the Agency;
- Attend meetings of the OMC on internal control;
- Recommend any new deficiencies for inclusion on the watch list and recommend closing deficiencies that have met milestones of their corrective action plan with verification and validation of results;
- Recommend a significance level for each newly identified deficiency and change the level as activities occur that raise or reduce the original significance. The three levels are:
    1. **Material Weakness (MW)** is defined as a deficiency in internal controls that is significant enough to be reported outside the Agency. The MW is the highest, most serious level of deficiency that may jeopardize the organization's mission.
    2. **Other Weakness (OW)** is the second level of deficiency that should be reported and monitored internally.
    3. **Management Challenge (MC)** is the lowest or least severe level of a major deficiency. The MC is defined as a concern about a challenge to management. There is insufficient information to confirm a serious systemic internal control weakness in this area. A MC may pertain to issues that are outside management's control or factors that may create an adverse condition. Close monitoring is required.
- Assess the fiscal year's final recommendations from the Senior Assessment Team on changing the watch list and decide on what material weaknesses to report in the annual Administrator's Statement of Assurance.

1.5.4 The Senior Assessment Team

The SAT is an arm of the OMC, which convenes under the direction of the Director for Program and Institutional Integration. Meetings of the SAT cover the latest information on planning and assessing the internal control program schedule, new risks, status of existing deficiencies on the OMC watch list, and the summary review to present at the OMC's year-end meeting on internal control. The SAT membership includes:

- Director of the Office of Program and Institutional Integration (Chairperson)
- Assistant Associate Administrator
- Deputy Chief Financial Officer (CFO)
- Associate Administrator of Institutions and Management
- Deputy Chief Engineer
- Deputy Chief Information Officer (CIO)
- Deputy Chief of Safety and Mission Assurance
- Deputy Associate Administrator for Aeronautics Research Mission Directorate
- Deputy Associate Administrator for Exploration Systems Mission Directorate
- Deputy Associate Administrator for Science Mission Directorate
- Deputy Associate Administrator for Space Operations Mission Directorate
- Deputy Center Directors (3 to serve on a rotational basis)

- Deputy General Counsel
- Deputy Inspector General (advisory capacity)

The Assistant Administrator for Internal Controls and Management Systems (OICMS) serves as the Executive Secretary to the SAT. The SAT integrates programmatic, financial, and institutional internal control across the Agency to ensure that internal controls are commensurate with identified risks and results-oriented management. The SAT strengthens coordination and communication in support of NASA missions and mission support offices and the Centers. The SAT convenes to:

- Provide leadership and oversight with respect to the Agency's internal control program;
- Review and approve internal control policies, programs, activities, and guidance associated with the annual Statement of Assurance process;
- Ensure effective senior management assessments of major deficiencies on the OMC Watch List, their significance level, root causes, corrective actions, verification and validation of corrections, target and final closure dates, and improvements to internal control;
- Report the status of Watch List deficiencies to the OMC and recommend new deficiencies, closure of deficiencies, and other changes;
- Assess progress of corrective actions taken to address identified control deficiencies;
- Develop and document, by Responsible Officials, the status of corrective actions and other key information about deficiencies and records of data officially maintained in the Agency's Corrective Action Tracking System (CATS);
- Report up to the OMC on recommendations for SOA certifications and the results of each year's internal control reviews;
- Advise the OMC on trends, deficiencies, and corrective actions;
- Ensure that information reported has been coordinated and integrated across programmatic, financial, and institutional lines.

1.5.5 Asst. Administrator for Internal Controls & Management Systems

The Assistant Administrator, Office of Internal Controls & Management Systems (OICMS) serves as NASA's lead for the Internal Control Program. Management activities include the following:

- Establish and maintain Agency policy for internal control;
- Ensure Agency compliance with the FMFIA and A-123 requirements;
- Report to the SAT on internal and external internal control activities;
- Provide management and staff support for the internal control program;
- Develop material in support of the annual call for Agency-wide SOA certifications;
- Coordinate material for the Administrator's Statement of Assurance;
- Develop and maintain web based links to key federal and NASA internal control references;
- Maintain an OMC Watch List of major deficiencies documented within the NASA CATS data repository for tracking corrections to various review findings and control issues;
- Maintain an internal control web site for records of meeting agendas, formal minutes, and briefings.

1.5.6 Officials-in-Charge and Directors of NASA Centers

The Officials-in-Charge (OICs) and Directors of NASA Centers have responsibility to:

- Implement internal control consistent with OMB Circular A-123 and in accordance with NPD 1200.1, NASA Internal Control;
- Actively support OMC and SAT meetings on internal control;
- Ensure the effectiveness of the internal control environment as implemented;
- Maintain and document internal control according to the GAO Standards for Internal Control in the Federal Government, which includes standards for control environment, risk assessment, control activities, information and communication, and monitoring;
- Promote the establishment of new or modified controls as needs arise and as identified by internal or external assessments;
- Provide resources to support internal control reviews/risk assessments and other types of internal or external review;
- Provide resources to mitigate identified risks;
- Report annually to the Administrator through the OICMS Assistant Administrator on the effectiveness of the organization’s internal control.

1.5.7 NASA managers and employees

NASA managers and employees, as stewards of Federal resources, have the following responsibilities:

- Operate within and improve their internal control environment;
- Participate in risk assessments of their internal controls;
- Report internal control deficiencies to the next management level;
- Correct internal control deficiencies;
- Ensure timely completion of assessment-related corrective actions;
- Ensure the reporting of all material weaknesses and other internal control deficiencies in the annual process for conducting control reviews;
- Report possible fraudulent, wasteful, abusive, or criminal activities to the NASA Inspector General (IG);
- Provide full and accurate responses to inquiries by internal or external auditors, review teams, or investigators, subject to legal restrictions.

1.5.8 The NASA Inspector General

The NASA Inspector General has responsibilities to:

- Oversee independent audits, investigations, and complaints regarding possible violations of law, fraud, waste, abuse, and other internal control deficiencies as set forth in NPD 9800.1, NASA Office of Inspector General Programs, based on mandates of the Inspector General Act;
- Serve as an ex officio member of the OMC, providing an independent perspective on identification, assessment, and closure of major deficiencies on the Council's Watch List;
- Serve in an advisory capacity on the SAT to provide an independent prospective on NASA’s internal control program.

Section 2: SoA Process Approach

2.1 Planning for the Annual Internal Control Review

The OICMS Assistant Administrator plans and develops the Agency-wide data call for conducting control reviews and submitting Statements of Certification. Planning is coordinated with the SAT. The planning and development process culminates with the SAT Chair's letter calling for all OICs and Center Directors to submit their Statements, using the evaluation tools in the ICP handbook as their source of requirements and standard templates.

In planning for the annual internal control review, OICs and Center Directors are responsible for:

- Updating the list/inventory of work activities and processes and information technology (IT) systems within their area of responsibility in terms of programmatic, institutional, and financial operations;
- Ranking in order of importance the identified work activities, processes, and IT systems using such criteria as the following:
    - Magnitude or limitation of resources
    - Susceptibility to fraud
    - Sensitivity of programs/functions
    - Level of integration or crosscutting programs and functions
    - Concern for safety and/or security
    - Policy issues
    - Issues with NASA and/or non-NASA support/liaison personnel
- Defining the control environment and performing initial risk assessments for all significant work activities, processes and IT systems identified. The risk assessment is a critical step in the process to determine the work activities, processes, and IT systems that need to be assessed during the annual internal control review and the extent of monitoring necessary over internal controls. Once the potential risks to achieving objectives of significant work activities, processes or IT systems have been identified, a risk rating of high, medium, or low should be assigned to each risk. The risk rating should take into consideration the inherent risk of not achieving objectives, the likelihood of the risk occurring, and the potential consequence or impact if the risk occurs. The initial risk rating should be based on no controls in place.

2.2 Conducting the Internal Control Review

2.2.1 Management is responsible for developing and maintaining internal control activities that comply with the following standards to meet internal control objectives:

- Control Environment,
- Risk Assessment,
- Control Activities,
- Information and Communications, and
- Monitoring

2.2.2 OMB Circular A-123 states that "management should have a clear, organized strategy with well-defined documentation processes that contain an audit trail, verifiable results, and specify document retention periods so that someone not connected with the procedures can understand the assessment process."

2.2.3 DOCUMENTING KEY WORK ACTIVITIES: OICs and Center Directors should document internal control activities to show how their significant activities, processes and IT systems are complying with the 5 internal control standards. The following in-depth description of standards should be considered:

2.2.3.1 CONTROL ENVIRONMENT: A positive control environment is the foundation for all other standards. It provides discipline and structure as well as the climate which influences the quality of internal control. Several key factors affect the control environment, including: The integrity and ethical values maintained and demonstrated by management and staff; management's commitment to competence; management's philosophy and operating style including the degree of risk the agency is willing to take; the attitude and philosophy of management toward information systems, accounting, personnel functions, monitoring, and audits and evaluations; the agency's organizational structure for planning, directing, and controlling operations; human capital policies and practices; and the agency's relationship with the Congress and central oversight agencies such as OMB.

2.2.3.2 RISK ASSESSMENT: A precondition to risk assessment is the establishment of clear, consistent control objectives. Risk assessment is the identification and analysis of relevant potential risks associated with achieving the objectives, and forming a basis for determining how risks should be managed. Management needs to comprehensively identify risks and should consider all significant interactions between the entity and other parties as well as internal factors at both the entity-wide and activity levels. Risk identification methods may include qualitative and quantitative ranking activities, management conferences, forecasting and strategic planning, and consideration of findings from audits and other assessments. Once risks have been identified, they should be analyzed for their possible effect. Risk analysis generally includes estimating the risk's significance, assessing the likelihood of its occurrence, and deciding how to manage the risk and what actions should be taken.

2.2.3.3 CONTROL ACTIVITIES: The policies, procedures, techniques, and mechanisms that enforce management's directives, such as the process of adhering to requirements for budget development and execution. Control activities occur at all levels and functions of the entity. They include a wide range of diverse activities such as approvals, authorizations, verifications, reconciliations, performance reviews, maintenance of security, and the creation and maintenance of related records which provide evidence of execution of these activities as well as appropriate documentation. Control activities may be applied in a computerized information system environment or through manual processes. Activities may be classified by specific control objectives, such as ensuring completeness and accuracy of information processing.

There are certain categories of control activities that are common to all agencies. Examples include the following: top level reviews of actual performance; reviews by management at the functional or activity level; management of human capital; controls over information processing; physical control over vulnerable assets; establishment and review of performance measures and indicators; segregation of duties; proper execution of transactions and events; accurate and timely recording of transactions and events; access restrictions to and accountability for resources and records; and appropriate documentation of transactions and internal control.

Also, there are two broad groupings of information systems control - general control and application control. General control applies to all information systems—mainframe, minicomputer, network, and end-user environments. Application control is designed to cover the processing of data within the application software.

General Control: This category includes entity-wide security program planning, management, control over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance. Data center and client-server operations controls include backup and recovery procedures, and contingency and disaster planning. In addition, data center operations controls also include job set-up and scheduling procedures and controls over operator activities. System software control includes control over the acquisition, implementation, and maintenance of all system software including the operating system, data-based management systems, telecommunications, security software, and utility programs. Access security control protects the systems and network from inappropriate access and unauthorized use by hackers and other trespassers or inappropriate use by agency personnel. Specific control activities include frequent changes of dial-up numbers; use of dial-back access; restrictions on users to allow access only to system functions that they need; software and hardware "firewalls" to restrict access to assets, computers, and networks by external persons; and frequent changes of passwords and deactivation of former employees' passwords. Application system development and maintenance control provides the structure for safely developing new systems and modifying existing systems. Included are documentation requirements; authorizations for undertaking projects; and reviews, testing, and approvals of development and modification activities before placing systems into operation. An alternative to in-house development is the procurement of commercial software, but control is necessary to ensure that selected software meets the user's needs, and that it is properly placed into operation.

Application Control: This category of control is designed to help ensure completeness, accuracy, authorization, and validity of all transactions during application processing. Control should be installed at an application's interfaces with other systems to ensure that all inputs are received and are valid and outputs are correct and properly distributed. An example is computerized edit checks built into the system to review the format, existence, and reasonableness of data.

Because information technology changes rapidly, controls must evolve to remain effective. Changes in technology and its application to electronic commerce and expanding Internet applications will change the specific control activities that may be employed and how they are implemented, but the basic requirements of control will not have changed. As more powerful computers place more responsibility for data processing in the hands of the end users, the needed controls should be identified and implemented.

2.2.3.4 INFORMATION AND COMMUNICATION: For an entity to run and control its operations, it must have relevant, reliable, and timely communications relating to internal as well as external events. Information is needed throughout the agency to achieve all of its objectives.   Program managers need both operational and financial data to determine whether they are meeting their agencies' strategic and annual performance plans and meeting their goals for accountability for effective and efficient use of resources. Pertinent information should be identified, captured, and distributed in a form and time frame that permits people to perform their duties efficiently. Effective communications should occur in a broad sense with information flowing down, across, and up the organization. In additional to internal communications, management should ensure there are adequate means of communicating with, and obtaining information from, external stakeholders that may have a significant impact on the agency achieving its goals. Moreover, effective information technology management is critical to achieving useful, reliable, and continuous recording and communication of information.

2.2.3.5 MONITORING: Internal control should generally be designed to assure that ongoing monitoring occurs in the course of normal operations. It is performed continually and is ingrained in the agency's operations. It includes regular management and supervisory activities, comparisons, reconciliations, and other actions people take in performing their duties. Separate evaluations of control can also be useful by focusing directly on the controls' effectiveness at a specific time. The scope and frequency of separate evaluations should depend primarily on the assessment of risks and the effectiveness of ongoing monitoring procedures. Separate evaluations may take the form of self-assessments as well as review of control design and direct testing of internal control. Separate evaluations also may be performed by the agency Inspector General or an external auditor. Deficiencies found during ongoing monitoring or through separate evaluations should be communicated to the individual responsible for the function and also to at least one level of management above that individual. Serious matters should be reported to top management.

2.2.4 ANNUAL SoA Review: The OIC or Center Director receives the data call for the annual internal control review and delegates the evaluation authority to managers directly responsible for the significant work activities and processes and information technology (IT) systems previously identified. The review of internal control involves managers and employees directly responsible for carrying out the activities or overseeing the processes or systems. Employees from other organizations, both internal and external, may participate on the review teams as authorized by management. At the immediate, actionable level, the "bottoms-up" teams of manager(s) and employees perform the internal control reviews and report the results to successive levels of management for their review and consideration. Upper level managers perform a "top-down" summary management review by considering the results of the reviews under their control along with other available information to determine which control weaknesses identified are reportable.

Some of the following methods may be used to determine that controls are operating properly:

- Sample documentation of the transactions using files, logbooks and other source documents
- Interview with staff on the procedures they follow to complete their tasks
- Observation of procedures/controls in action
- Testing to check if backups work

Below is a partial list of important types of audits, reviews, and assessments conducted at NASA. Pertinent reviews should be collected and compared to the results of the self assessments of internal controls to substantiate the assessments.

1. Program/project management reviews (such as Preliminary Design Review and Critical Design Review) as required by NASA Procedural Requirements 7120.5, NASA Program and Project Management Processes and Requirements.
2. Internal surveys, audits, and reviews initiated by Headquarters (such as Procurement Management Survey) as defined in NASA Policy Directive 1210.2, NASA Surveys, Audits, and Reviews Policy.
3. Council assessments such as Program Management Council reviews.
4. Engineering or scientific peer reviews.

5. Safety and mission assurance reviews as covered in NASA Procedural Requirements 8705.6, Safety and Mission Assurance Audits, Reviews, and Assessments.
6. Mishap investigations as described in NASA Procedural Requirements 8621.1, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping.
7. Security reviews as defined in NASA Procedural Requirements 1600.1, NASA Security Program Procedural Requirements.
8. Information technology security assessments as documented in NASA Procedural Requirements 2810.1, Security of Information Technology.
9. Quality control reviews.
10. Risk assessments as defined by NASA Procedural Requirements 8000.4, Risk Management Procedural Requirements, NASA Procedural Requirements 8705.5, Probabilistic Risk Assessment Procedures for NASA Programs and Projects, and NASA Procedural Requirements 7120.5.
11. Financial management reviews as documented in the NASA Financial Management Requirements, Volume 9, Internal Management Controls.
12. Management system audits, internal and external, as required by NASA Policy Directive 1280.1, NASA Management System Policy.
13. Internal audits or self-assessments initiated by management at Centers/Headquarters.
14. Standards, operations, and workload reviews.
15. Configuration control board reviews.
16. Contractor performance reviews.
17. NASA personnel performance plans and reviews.
18. Inspector General audits and investigations.
19. Government Accountability Office audits.
20. Defense Contract Audit Agency audits.
21. Reviews by independent non-NASA entities such as other Government agencies or specially assigned panels such as the Columbia Accident Investigation Board.

2.2.5 Once the SoA reviews are completed, the residual risks to achieving objectives of significant work activities, processes or IT systems should be assigned a level of high, medium, or low. The revised risk rating should take into consideration whether mitigating internal controls have been placed in operation and are functioning as intended. The following definitions are to assist with rating risks:

Low: No indication of material weaknesses or internal control failures. There is evidence that the established internal controls are functioning as intended.

Medium: More serious than a low rating because of evidence of weakness in internal controls. There are indications that internal controls are not functioning as intended (e.g., regular reports are not being produced; a missing level of management oversight is identified; security violations do or can easily occur; escalating costs are documented but not yet fully funded).

High: Indications of serious material weaknesses or internal control failures. There is significant evidence that needed internal control activities do not exist or are not functioning substantially as intended (e.g., key program/project milestones are consistently not being met; inadequate facilities/equipment/software are consistently not funded for update/correction; contract products and services are not regularly reviewed for contract compliance, quality, safety, and security).

INTERNAL CONTROL Evaluation Tool: A sample tool for documenting compliance with internal control standards is provided in Section 3.2. For the significant activities, processes and IT systems identified, OICs and Center Directors should ensure the internal control evaluation tool is completed. Care should be taken to not duplicate documentation already available to support compliance with OMB

Circular A-123, Appendix A, as it pertains to controls over financial reporting, including controls over financial IT systems.

2.2.6 OIC AND CENTER DIRECTOR STATEMENT OF CERTIFICATION: As deficiencies are reported to upper management, judgments of significance level are made by progressively senior managers with a broader perspective of NASA's missions and functions. High risks must be tracked until corrected. Managers must consider whether the deficiency ranks as a material weakness, which by law must be reported externally. The following criteria may assist in classifying a deficiency at the material weakness level:

- Substantially impairs the organization's performance, mission, and strategic direction
- Violates statutory or regulatory requirements
- Substantially weakens safeguards against waste, loss, unauthorized use, and misappropriation of funds or other assets
- Results in a major conflict of interest
- Indicates significant security or safety concerns
- Exists in a majority of programs, administrative functions, and/or organizations and can cause harm, though seemingly minor individually, because the aggregate is significant

The ICP checklist/survey found in Section 3.3 should be used by OICs and Center Directors to summarize and document results of reviews of all significant work activities, processes or IT systems for which they are responsible. This scorecard contains questions pertaining to each of the internal control standards that should be answered by choice of a green (good), yellow (acceptable but needs some attention), or red (none or negligible confidence of internal control).

2.2.7 Based on the results of the reviews as summarized in the checklist, the responsible OIC or Center Director signs a transmittal memorandum certifying the organization's type of Statement of Certification (See Section 3.4). The 3 types of Statements are unqualified, qualified, or no assurance. These types are described as follows:

1. **An unqualified Statement of Assurance** explains that sufficient controls are in place and effectively working. This Statement of reasonable internal control assures management that there are no material weaknesses to report. Each unqualified Statement shall provide a sound basis for that position, and the effectiveness of controls will be summarized in the cover memorandum.

2. **A qualified Statement of Assurance** means that there is reasonable assurance of internal control with the exception of one or more material weaknesses. The number of material weaknesses must be cited and briefly described in the cover memorandum as illustrated in Section 2.4.

3. **A Statement of No Assurance** is simply a negative statement meaning that the head of the organization does not have reasonable assurance of the effectiveness of internal control. No Assurance indicates a lack of internal control processes in place or pervasive material weaknesses. The basis for this position shall be summarized in the cover memorandum, and each material weakness shall be documented according to the template in Section 2.3.

The original signed hardcopy Statement of Assurance certification (sample provided in Section 3.5), the ICP checklist, and any accompanying information are to be submitted by **July 31** of each year to the Administrator through the Assistant Administrator for Internal Controls and Management Systems. An electronic copy is provided to primary staff members: Mike McFadden Michael.mcfadden@nasa.gov, John Werner john.d.werner@nasa.gov and Marie Tynan marie.k.tynan@nasa.gov.

2.3 Analysis of Certifications by OICMS Team and the SAT

The goal of the internal control review methodology is to provide an effective evaluation of SoA Certifications submitted each year by OICs and Center Directors. The OICMS Internal Control Team will evaluate all available information to identify new and determine the status of prior internal control deficiencies. The Team Lead briefs the OICMS Assistant Administrator before the formal presentation is made to the SAT for a higher level analysis of the findings. The SAT coordinates the final evaluation briefing with the Deputy Administrator, other senior officials from the Office of the Administrator, the Office of Institutions and Management, the Office of the Chief Financial Officer, and others as needed.

2.4 OMC Decision Process

At the annual decision meeting of the OMC on internal control, the SAT Chairperson and the OICMS Assistant Administrator brief the council on the SAT recommendations of any material weaknesses to report and other deficiencies that should be considered for closure, change in significance level, or addition to the watch list at lower significance levels for internal tracking. The summary level charts provide the SAT recommendations as to the evidence requested by the Administrator to support his position on the NASA Statement of Assurance certifying the status of internal control throughout the Agency. The OMC Chairperson, council members, and the Inspector General assess the briefings and may ask questions, debate opinions, and introduce further evidence to make an informed judgment on the material weaknesses to be reported and any changes to be made on the deficiency watch list. The OMC Chairperson then decides on the addition, deletion, and significance level changes of deficiencies on the watch list. Officials responsible for material weaknesses brief the OMC on recommendations pertaining to correct their material weaknesses.

2.5 Administrator's Statement of Assurance

The Administrator's Statement of Assurance is a legal document required since 1982 by the Federal Managers' Financial Integrity Act. It is similar to an annual report in industry that is introduced and signed by the President or Chief Executive Officer explaining how the company performed over the year including financial statements. In government, the Statement of Assurance is provided by November 15 of each year and included in every agency's ***Annual Financial Report***, distributed to OMB, Congress, and the President.

In NASA the Office of Internal Controls and Management Systems provides staff to draft the Administrator's Statement shortly after the OMC year-end decision meeting. Documentation from material weakness owners is provided to the OICMS according to a tight deadline. The complete draft is presented to the SAT for review and modification as necessary. When the final draft is completed, the OICMS staff is responsible for providing the electronic copy to support staff of the ***Annual Financial Report*** for integration of the Statement into the overall annual report.

2.6 Follow-up on Correcting Deficiencies and Monitoring Progress

NASA internal control deficiencies are distinctly separated into (1) major deficiencies on a watch list monitored by the OMC and (2) all other high, medium, and low deficiencies monitored by the SAT with status reports on corrective actions given to close OMC watch list issues and lower level deficiencies considered significant by the SAT membership. The OMC meets annually to assess the status of corrective actions for closing major deficiencies on the watch list. A web site with documentation of SAT meetings is managed by staff to the OICMS Assistant Administrator. The Agency internal control corrective action tracking system is also managed by OICMS staff. Data fields of the online tracking system include deficiency title, description, root cause, corrective action plan, quarterly status of corrective actions taken, target correction date, measures, validation, and a place for adding links to references (policy, other reviews, plans, etc.) pertaining to the identified deficiency. Definitions of these data fields appear in Section 3.5 on the template for documenting material weaknesses. Each deficiency on the OMC watch list is assigned for correction to the responsible senior official at Headquarters or Center Director.

OICs and Center Directors responsible for high risks not on the OMC watch list should appoint an official internal to the organization for taking immediate and/or long term actions that will eliminate or mitigate the internal control deficiencies. The responsible official should develop a corrective action plan similar to the summary level template for material weaknesses. Each corrective action plan should be scoped and written based on the complexity of the deficiency. The responsible official may call on internal or external parties for assistance in monitoring the deficiency to closure. Final closure should be reported to the organization's OIC or Center Director. Deficiency closures should occur before the next internal control review begins or they must be reported along with the status of new deficiencies.

Section 3: ICP Required Documents & Examples

3.1 Statement of Certification Evaluation Tools

The ICP Handbook establishes standard assessment tools for use in evaluating and reporting results of a NASA SoA Certification process. The internal control evaluation tool in Section 3.2 is used to document internal control activities in place for key work activities, processes and IT systems. The evaluation tool documents how the 5 GAO standards for internal control are being met. A risk level of high, medium or low must be assigned to each key activity, process or IT system identified. The second evaluation tool (Section 3.3) is a checklist for NASA OICs and Center Directors to use in certifying how well NASA internal controls are implemented. The scoring method requires a Red/Yellow/Green or Not Applicable mark for each of the questions in the checklist. The definitions (3.4) for identified deficiencies that become part of the OMC watch list are presented for reference and may be used to propose a new material weakness and/or recommend other deficiencies that should be tracked internally on the watch list. Material weakness is the highest level of reportable risk with other deficiencies on the watch list rated as Other Weakness and Management Challenges. A template for material weaknesses (3.5) is used at the discretion of the OIC or Center Director for a deficiency rated at the high risk level. The standard letter for transmitting the certification of review results is presented in Section 3.6.

This Page Left Blank

3.2 Sample (Organization) Internal Control Evaluation Tool

Control Objective	Work Activity	Control Environment	Risk Assessment	Risk Rating	Control Activities	Information and Communications	Monitoring
Fly the Shuttle as safely as possible until its retirement, not later than 2010.	Certification testing of Space Shuttle Main Engines and other tests to meet Shuttle manifests.	Chain of command clearly defined; Management encourages opposing views; Suitable hierarchy for reporting and schedule through 2010 established; CAIB Report findings used for continual improvements.	Not meeting required test certification dates that could delay Space Shuttle activities due to scheduling issues or last minute test requirements.	M	Compliance with NPR 7120; Rigorous testing and technical reviews; Strong coordination between HQ and Centers; One full time person managing this program. Risk management is built into the selection of contract type and administration strategies for on going procurements.	Formal system requirement reviews and design reviews are held and there are various Configuration Control Boards. Data is accessible through Windchill. Monthly contract reviews are held.	The 9001/14001 Management System is in place as well as the Office of Quality Assurance periodic monitoring of controls and their annual audits.
Ensure that the ATP wind tunnels safely produce high quality data in support of program requirements.	Operate ATP wind tunnels effectively and safely.	Clear roles and responsibilities between NASA and contract operator. Robust staffing plan to maintain government strategic responsibilities and stewardship. Extensive contract operator training plan.	Broken or poorly operating systems will prevent the delivery of program milestones and will affect overall quality of data	M	Constant attention to safety of test hardware and facility. Prioritization of maintenance and facility upgrades. Tracking of component certifications. Compliance with LPR 1710.10,1710.15,1710.40, 1710.42, 1740.2; Use of Standard Practice Engineers to insure consistent best practices: LMS-CP-0502, “Wind tunnel Planning”; LMS-CP-0504 ” Conducting a wind tunnel test”; LMS-CP-0505, “Closing out a wind tunnel test.”	Regular meetings within each facility. Weekly meetings within the directorate. Financial information communicated to all facilities. Facility input on prioritization of maintenance and upgrades. Monthly facility manager/facility safety head meetings.	Customer feedback acquired on all tests. Monthly tracking of financial data including spending metrics. Pre-test safety reviews. Regularly review under-maintained research systems and supporting infrastructure” Recent examples of this are: 1. failures at the Compressor Station; 2. failure of high energy rotating equipment at UPWT; 3. UPWT compressor leaking oil into test medium resulting in unacceptable data quality.

Establish and maintain integrated NASA program and project management policies, governance and tools which support the portfolio of Agency-wide programs and projects.	Program and Project Management provides Agency policy, governance, and tools to enable the successful management of NASA programs and projects.	Coordination and Implementation through the Center and Mission Directorate representatives on boards and working groups including the Program/ Project Management Board (PMB) and the Earned Value Management Working Group (EVMWG)	Failure in program and project management would negatively impact Agency resources which could contribute greatly to loss of missions. Without the full implementation and support coming from program and project management the project is exposed to excessive risk.	High –	NASA Policy Directive (NPD) 7120.4C, NPR's 7120.5D, 7120.7, 7120.8 and related handbooks.	Establishment of Baseline Performance review and evaluation process coordinated with Design Reviews Program/Project On-line Library And Resource Information System (POLARIS) Engineering Management Board Meetings Program and Project Management Board BPR automation Weekly Staff meetings	Monthly Status Review of technical and budgetary performance Baseline Performance Review (BPR) Center implementation Surveys
Ensure effective oversight of outsourced work	Contract/ Grant Management and Administration	Statutory, Federal and Agency-level acquisition guidance. Established organizational structure with defined areas of authority and responsibility. Programmatic/ Acquisition activities aligned with Agency strategic direction and programs.	Non-compliance w/Federal Acquisition Regulation, the NASA FAR Supplement and Procurement/Grant Information Circulars during contract administration has wide-ranging impacts and potential penalties. Failure to closely monitor contractor performance may lead to payments for work not performed, work performed that is outside contract scope, untimely deliverables or deliverables not in compliance with contract requirements, and cost overruns.	H	Timely communication and implementation of new statutory and/or federal requirements to Center personnel. Dedicated HQ analyst assigned to each Center; level of review and oversight for each acquisition determined by dollar value and/or complexity. HQ focal point for each area of the FAR and NFS. Training conferences for Procurement personnel from all Centers and HQ Procurement Strategy Meetings for applicable acquisitions. On-line tool (Virtual Procurement Office) maintained by HQ to provide current guidance for file documentation. Comprehensive training and certification program for 1102s. Requirement for continuous learning courses/points (80 hours every two years) for all 1102 personnel.	Monthly Procurement Policy telecon with center reps in dialogue with HQ Procurement to discuss policy issues and answer questions from the Centers. Training conferences for Procurement personnel from all Centers and HQ. Procurement Strategy Meetings for applicable acquisitions. Pre- established e-mail distribution lists to Center Procurement management (with built-in redundancy) to instantly disseminate critical information. NASA Procurement Library accessible to all NASA personnel. Customer training on important issues and procurement changes.	Management Surveys; Center Self-Assessment; Procurement Officer one-on-one with AA for Procurement; Monthly Baseline Performance Review reporting; Monthly Undefinitized Contract Action (UCA) reporting; IG/GAO Audits. Customer surveys and customer visits.

Ensures information system security across the enterprise.	Develops and maintains information security programs. Develops a frame work for organizing consistent security policy. Develops privacy management procedures. Coordinates the design and implementation of processes and practices that assess and quantify risk.	Areas of authority and responsibility are clearly defined; Suitable hierarchy for reporting is established; Management responsive to implementing new federal requirements.	Systems may not be in compliance with regulations. System changes and associated risks may not be fully known and vetted putting systems at increased risk of compromise. Resources may not be adequate to complete all monitoring activities within the required timeframes. Lack of reliable and timely information of arrivals and departures of employees and contractors. Resources may not be adequate to properly investigate all incidents and determine/ implement required mitigating factors. Failure to adequately document systems and configuration and restoration timelines may cause delays in recovery from a contingency event.	H	Internal Controls program to include threat assessment, situational awareness, and proactive assessments; POA&M being given significant OCIO senior management attention. Annual review and update of processes and procedures. IT Security Program Management Office roles and responsibilities being completed. Security Operations Center for incident management and response being completed. Enterprise encryption for Data at Rest solution selected and being implemented. POA&M database being updated and reported on a monthly basis. Federal Desktop Core configuration being implemented. Continuous monitoring of NASA information systems and certification and accreditation as needed. Annual E-gov Privacy compliance verification of NASA registered Web sites using the AWRS system.	OCIO staff meetings. IT Security Managers weekly telecom. Quarterly ITSM workshops. Weekly transition planning meetings with NASIRC (NASA Incident Reporting Center). Outreach meetings with Centers, OIG, and HQ Mission Support and Mission. Directorate offices Monthly reporting of Centers' high vulnerabilities. Weekly one hour training sessions to Centers on pertinent topics such as FDCC reporting. Weekly incident telecom. Weekly C&A telecom. Technical team meetings. Generate XML reports for OMB. Biweekly Privacy Act Manager teleconference Privacy Act Training module in Satern.	OCIO Action tracking registry. C&A tracking system. POA&M tracking system. Ongoing vulnerability scanning using NASA scanning tool. Continuous Monitoring NITR (NASA IT Requirements) document. Contingency Plan testing and SOP updates. IT Security performance metrics and reporting. Privacy Impact Assessments (PIAs) of information systems, Web sites and information collections.

This Page Left Blank

3.3 Key Objectives Checklist

The items in this checklist reflect key NASA internal control objectives; i.e., organizational and procedural responses to previously identified programmatic, institutional and IT system risks. This list is intended to complement other, generic checklists such as the General Accountability Office's Internal Control Management and Evaluation Tool.

Each of the following questions or combination of questions should be considered in completing your Certification of Reasonable Assurance. Specifically, please respond to each question or combination of questions with marking Green, Yellow, Red, or Not Applicable, using the following definitions:

- **Green. You can generally answer "yes" for your organization and there are no known related internal control deficiencies.**

- **Yellow. You can generally answer "yes" for your organization, but there are known related control deficiencies; or, you can not answer "yes" for your organization but there are no significant known control deficiencies as a result.**

- **Red. There are significant known control deficiencies.**

- **Not Applicable. The question does not apply to your organization.**

For questions rated red or yellow, additional detail on the control deficiency should be provided to OICMS. If Green, supporting information, such as examples of reviews, assessments, and other management or external activities that support this assessment, should be available to OICMS upon request.

[NOTE: The Office of Internal Controls and Management Systems has developed a web-based capability for each organization to use in responding to this checklist. The address is http://nodis-dms.gsfc.nasa.gov/coc_survey/coc_surveyform.cfm.

Point of Contact/Phone Number:

Control Environment	**Green**	**Yellow**	**Red**	**N/A**	**Comment**
1. Do you have the requisite supporting capabilities (i.e., workforce, infrastructure, and information systems) required to successfully meet your programmatic and functional objectives?					
2. Does your organization employ, or is it subject to, sufficient independent or non-advocate assessments to ensure objectivity and outside perspective in the design, operation and measurement of programmatic and functional activities?					
3. Does your organization conduct periodic analyses of the knowledge, skills and abilities needed to accomplish your mission?					
4. Does your management foster and encourage an organizational culture that emphasizes the importance of integrity and ethical values?					
5. Do your employees possess the requisite skills and competencies required to successfully perform their duties?					
6. Do you provide to, or enable access to, the training and development activities that are required to maintain the technical, managerial, and functional excellence required to be successful in achieving its mission?					
7. Do you establish clear performance plans and objectives for your employees, and do you measure, reward, and - where necessary - discipline employees based on those plans?					

8. Does your organization have in place sufficient activities and controls to appropriately protect the public, the NASA workforce, and high-value equipment and property from potential harm as a result of NASA activities and operations?	🟩	🟨	🟥		
9. Does your organization assign duties and responsibilities such that no one individual can inappropriately control all aspects of an activity or event, and do you conduct checks to ensure that this is the case?	🟩	🟨	🟥		
10. Do you have reasonable assurance that employees within your organization receive required annual ethics training?	🟩	🟨	🟥		
11. Within your area of responsibility, do you have a recognized governance structure that enables the identification, assessment, reporting, and resolution of management related issues across organizational and functional boundaries? For example, are the processes for decision-making and appeals working as intended?	🟩	🟨	🟥		
12. Within your area of responsibility, do you have an established organizational structure with delegated, clearly defined, and documented areas of authority and responsibility? Do you periodically evaluate that structure to make necessary changes in response to changing conditions?	🟩	🟨	🟥		
13. Do you clearly communicate to your employees the standards for acceptable behavior and the consequences for improper conduct?	🟩	🟨	🟥		
Risk Assessment					
14. Are your programmatic activities aligned with the Agency's strategic direction and/or are your functional activities aligned with the Agency's programs?	🟩	🟨	🟥		

15. Do you have clearly established goals, objectives, and/or mission success criteria for each of these programmatic and functional activities? Are these goals, objectives, and/or criteria available in written form, and are they clearly communicated to employees?	🟩	🟨	🟥		
16. Are you assessing the effectiveness and efficiency of your program/functional activities? For example, do you regularly review actual performance against plan, including an examination of budgets, forecasts, and prior period results?	🟩	🟨	🟥		
17. Within your organization, do you have a method to comprehensively and continuously identify and prioritize internal and external risks to achieving your goals and objectives?	🟩	🟨	🟥		
18. Once risks are identified, do you have a process to analyze and manage each risk, including assessments of the likelihood, consequence and potential mitigating strategies associated with each risk?	🟩	🟨	🟥		
19. Do you incorporate information from external audits (e.g., GAO and OIG) and internal surveys, assessments and reviews into your program/functional reviews, risk assessments, management controls, and corrective actions on a timely basis?	🟩	🟨	🟥		
20. Is your organization in compliance with known external and internal statutes, regulations, policies, directives, and standards, and other similar requirements?	🟩	🟨	🟥		
21. Do risk identification and discussions occur in senior level management conferences?	🟩	🟨	🟥		
Control Activities					
22. Do you prepare corrective action plans to ensure remediation of control weaknesses and deficiencies, and do you track the completion of such actions?	🟩	🟨	🟥		

23. Are all reviews/boards and similar review activities conducted by or within your organization well-defined and planned?	🟩	🟨	🟥		
24. Do you have approved budget execution plans or similar documents for programs and/or functional activities within your area of responsibility that clearly identify when, where and what resources are to be applied to each program/activity?	🟩	🟨	🟥		
25. Are funds released and applied in accordance with these budget execution and similar plans, as well as consistent with other existing guidance and constraints?	🟩	🟨	🟥		
26. Does your organization have a process to re-allocate resources across programmatic and functional activities to maintain an optimum alignment with Agency and organizational goals and objectives?	🟩	🟨	🟥		
27. Does your organization have an established process for performing inspection and acceptance of contractor deliverables prior to final payment?	🟩	🟨	🟥		
28. Does your organization employ sufficient controls to ensure physical control over vulnerable assets? For example, do you have an established process for issuing, tracking, and recovering government furnished property and equipment, and does your organization periodically compare your physical assets with data recorded in inventory and financial systems, and examine any discrepancies?	🟩	🟨	🟥		

29. Does your organization employ sufficient controls to ensure that all activities are performed by authorized personnel? For example, does your organization employ sufficient controls to limit access to sensitive information, including Personally Identifiable Information, where required?	🟩	🟨	🟥		
30. Does your organization effectively manage the workforce through a clear and coherent vision of the Agency's mission, goals, values, and strategies?	🟩	🟨	🟥		
31. Does your organization employs a variety of control activities suited to information processing systems to ensure accuracy and completeness?	🟩	🟨	🟥		
32. Does your organization have established performance measures and indicators, which are periodically reviewed for effectiveness?	🟩	🟨	🟥		
33. Do you document your risk assessment, monitoring/testing, and other internal control activities? Is this documentation adequate to easily explain your internal control efforts to someone who is not connected with your procedures, and to support your certification of reasonable assurance?	🟩	🟨	🟥		
Information and Communication					
34. Does your organization have adequate mechanisms to enable the timely flow of contractor cost and schedule data to decision makers?	🟩	🟨	🟥		
35. Do you make it clear to your employees that there will be no reprisals for reporting adverse information, improper conduct, or circumvention of approved activities?	🟩	🟨	🟥		

36. Do you encourage your managers and employees to identify and report on potential programmatic and functional risks, as well as potential internal control deficiencies or other weaknesses? Is there evidence that such reporting is occurring?	🟩	🟨	🟥		
37. Do employees have a means of communicating information upstream within your organization, including through someone other than a direct supervisor?	🟩	🟨	🟥		
38. Does your organization have adequate mechanisms to enable the flow of information, down, across, and up the organization? Is open communication evident, with all parties having an opportunity to be heard?	🟩	🟨	🟥		
39. If your organization is responsible for establishing policies, procedures, standards or other guidance for other organizations, are these policies, procedures and/or standards clearly written and adequately disseminated?	🟩	🟨	🟥		
40. If your organization is responsible for establishing policies, procedures, standards or other guidance for other organizations, do you have a process to determine if these policies, procedures and/or standards are accessible to all who need to know and are actually being followed?	🟩	🟨	🟥		
41. Does management ensure that effective external communications occur with customers, suppliers, contractors, consultants, and other groups that can provide significant input on quality and design of agency products and services?	🟩	🟨	🟥		
42. Does your organization make decisions with adequate technical analysis, guidance, and input?	🟩	🟨	🟥		
43. Do decision makers have access to all required data?	🟩	🟨	🟥		

Monitoring					
44. Are program and/or other documents required by Agency and/or Center policy complete and in place?	🟩	🟨	🟥		
45. Does your organization conduct periodic analyses of the supporting infrastructure (facilities, information technology, etc.) needed to accomplish your mission?	🟩	🟨	🟥		
46. Does your organization have access to the infrastructure required to successfully accomplish your programmatic and functional responsibilities?	🟩	🟨	🟥		
47. Is your supporting infrastructure maintained at an appropriate level to ensure that required capabilities are available in a timely and safe manner when needed for use by programmatic and functional activities?	🟩	🟨	🟥		
48.Does your organization conduct ongoing monitoring and reporting that provide reasonable assurance that controls are working as intended?	🟩	🟨	🟥		
49. Are results of internal or external evaluations used to ensure controls are working as intended? For example do review results trigger additional testing or separate assessments where major problems are identified?	🟩	🟨	🟥		
50. Do you use information obtained during program/functional reviews, risk assessments, and similar activities to identify internal control weaknesses and deficiencies?	🟩	🟨	🟥		

3.4 Definitions of OMC Watch List Deficiencies

TITLE	DEFINITION	REPORTING
Material Weakness	A control deficiency, or a combination of deficiencies, that may jeopardize the accomplishment of the Agency's mission, result in repeated violations of statutory or regulatory requirements, and/or significantly weaken safeguards against waste, loss, unauthorized use, or mismanagement of Agency assets.	Weaknesses and summaries of corrective actions reported externally with SOA signed by Administrator
Other Weakness	A control deficiency, or a combination of deficiencies, that – if not addressed – has the potential to jeopardize the accomplishment of the Agency's mission, result in repeated violations of statutory or regulatory requirements, and/or significantly weaken safeguards against waste, loss, unauthorized use, or mismanagement of Agency assets.	Internal to the Agency
Management Challenge	A control deficiency, or a combination of deficiencies, that has, or has the probable potential for, substantive negative impact on the effectiveness and/or efficiency of Agency operations, decreased reliability of financial reporting, and/or compliance with applicable laws and regulations.	Internal to the Agency

3.5 Material Weakness Template

Include this template when a material weakness is identified:

Title: (Assign a descriptive title to the material weakness.)

Responsible Official: (Enter name, title, and organization of senior official accountable for corrective action -- OIC or Center Director.)

Description: (Summarize the deficiency in terms of its effect on mission accomplishment, cost impact, compliance impact, schedule slippage, operating efficiency, etc. Cite the single or multiple NASA organizations involved.)

Root Cause(s): (Explain the one or more factors [events, conditions, or organizational factors] that contributed to or created the direct/immediate/proximate cause and subsequent undesired outcome and, if eliminated or modified, would have prevented the undesired outcome.)

Corrective Action Plan (CAP): (Summarize the proposed strategy/approach or course of action to correct the deficiency. Describe the corrective actions along with a designation of the organization[s] responsible for implementing the corrective actions and a completion date for each corrective action. If available, cite the Web site for access to detailed documents with short-term actions, longer-term goals, and completed actions.)

Target Correction Date: (Enter projected date for correction of all actions.)

Results/Measures for CAP: (Briefly describe what measures will be used to evaluate whether actions taken have corrected the root/underlying cause of the deficiency. Measures must be based on observable performance metrics -- qualitative, quantitative, or both.)

Validation Process: (Describe how results/measures will be or have been subjected to verification and validation. Examples of validation approaches may include use of existing program, project, and other management reports; business data, survey data, sampling/analysis data; internal and/or external assurance reviews, audits, interviews, and other NASA-established Independent Verification and Validation tools and techniques.)

3.6 Template for Certification Letter

OMB Circular A-123 addresses three types of Government-wide assurance statements. Each NASA letter of certification provides a statement of assurance, which applies to the organization – unqualified, qualified, or no assurance. These three types are defined in this template for certification.

Template for Certification Letter

TO: Administrator

THRU: Assistant Administrator, Internal Controls and Management Systems

FROM: **Center Director (or Official-in-Charge)**

SUBJECT: FY2008 Certification of Reasonable Assurance Over Internal Control

As the **(Title)** of **(Center/Organization),** I recognize that I am responsible for the implementation of internal controls within my area of management responsibility consistent with NASA policy, and in particular in accordance with OMB Circular A-123 and the Government Accounting Office's Standards for Internal Control in the Federal Government.

As a result of our ongoing internal control activities, and in particular those activities that have been in place and operational during the current fiscal year, I am able to provide... **[choose from one of the following]:**

- ...an unqualified certification of reasonable assurance over internal control. **[To be used if there are no control deficiencies, or combination of deficiencies, present that may jeopardize the accomplishment of your organization's mission, result in repeated violations of statutory or regulatory requirements, and/or significantly weaken safeguards against waste, loss, unauthorized use, or mismanagement of your organization's assets. Please describe the risk assessment, management review, and other internal control elements in operation within your organization that provide support for your assertion of an unqualified certification. In particular, you should provide a summary of significant findings from reviews and corrective actions taken to improve internal control during FY2008. Also, state that you have reviewed each of the key control objectives in the checklist provided by OICMS and that each of these objectives is currently being met.]**

- ...a qualified certification of reasonable assurance over internal control. **[To be used if there are control deficiencies, or combination of deficiencies, present that may jeopardize the accomplishment of your organization's mission, result in repeated violations of statutory or regulatory requirements, and/or significantly weaken safeguards against waste, loss,**

unauthorized use, or mismanagement of your organization's assets. Please describe the basic risk assessment, management review, and other internal control elements in operation within your organization, and then summarize the control deficiencies that prevent you from providing an unqualified certification. Also, state that you have reviewed each of the control objectives in the checklist provided by OICMS as part of the deliberations leading up to the completion of your certification.]

- ....no certification of reasonable assurance over internal control. **[To be used if there are no processes in place to assess internal control, or if there are pervasive control deficiencies, or combinations of deficiencies, present that jeopardize the accomplishment of your organization's mission, result in repeated violations of statutory or regulatory requirements, and/or significantly weaken safeguards against waste, loss, unauthorized use, or mismanagement of your organization's assets. Please provide a listing of the significant control deficiencies that exist within your organization, and describe the actions that are being taken to address these deficiencies, as well as to establish an appropriate internal control regime.]**

In addition, I would like to take this opportunity to submit the following issues for consideration by the Senior Assessment Team and the Operations Management Council for addition to the Agency's watch list as a Material Weakness, Other Weakness, or Management Challenge:

(Each issue should include a title and description of the proposed deficiency, plus any additional information that the Center or Headquarters Office may wish to provide regarding root cause, responsible organization, and proposed corrective actions. Please note that these issues do not have to be limited to issues for which the signatory's organization is responsible.)

If you have any questions regarding this certification, please contact **(please provide the name and telephone number of a point-of-contact)**.

(Signature of Center Director or Official-in-Charge)

Section 4: Examples of Programmatic, Financial, and Institutional Work Activities, Processes and Cycles

4.1 Programmatic Examples

Provide Program Management policy, direction, implementation, assessment and oversight (Overarching Policy, NPR 7120) (OCE)
Provide policy guidance for NASA Software Engineering Requirements by NPR 7150.2 (OCE)
Provide policy guidance for NASA Systems Engineering Requirements per NPR 7123.1A (OCE)
Maintain an Integrated NASA Technical Standards System to provide Agency Wide Access to Standards and promulgate Technical Standards guidance per NPD 8070.6. (OCE)
Manage the NASA Technical Fellows Program (OCE/NESC)
NASA Engineering Network (OCE)
Manage the Academy for Program, Project and Engineering Leadership (APPEL)(OCE)
Manage the process for Communication of Lessons Learned per policy NPR 7120.6 (OCE)
Management of Inventions and Contributions (OCE)

Perform Independent Cost Estimating and Standards (PA&E)
Evaluation of Mission Programs and Projects (PA&E)
Integrate NASA’s Strategy, Programs and Budget (PA&E)
Perform studies and assessments (PA&E)
Coordinate Annual Performance Plans and Reports in accordance with Government Performance and Results Act (GPRA) (PA&E)

Safety Oversight (OSMA)
Mission Assurance Oversight (OSMA)

Contract management at JPL and APL (OPII)
Management of Deep Space Network Contracts for Governments of Spain and Australia (OPII)
Manage Corporate G&A, Institutional Investments and CMO Budgets (OPII)
Oversight of Reimbursable Contract activity at the Centers (OPII)
Oversight of Sponsored Research and Education contract (OPII)

Technology Transfer (IPP)

Export Control Program (OER)

Oversight of the Flight Program (NASA Strategic Goal 3) (SMD)
Oversight of the Research and Analysis Program (SMD)

Next Generation Air Transportation System (ARMD)
Aeronautics Research (ARMD)

Oversee the formulation, definition and maintenance of Level 1 requirements (ESMD)
Maintain ESMD Program/ Project Management and Status Reporting Structure

Launch Services (SOMD)
Space Transportation (SOMD)
Space Communications and Navigation (SOMD)
Rocket Propulsion (SOMD)
Human and Robotic Exploration (SOMD)

Conduct Basic (Fundamental) Research
Conduct Applied Research
Perform Flight Research projects
Scientific Research

Space Shuttle Main Engine Testing
On-Orbit Data Support for 747 Carrier Operations
Flight Platform to Support Space Telescope Operations
Manage Flight Operations
Modify Research Aircraft to support Project requirements
Hardware Production
Facilities Testing
Testing of Technical Systems
Software and Engineering Development
System Engineering
Operate ATP Wind Tunnels
Transition to support the next generation of Exploration and Science Programs
While safely flying out the Shuttle and completing the ISS

Safety and Facility Assurance
Mission Assurance: (e.g., Design, Software and Flight)
Quality Assurance (e.g., Fabrication and Assembly Inspections; Material Analysis and Quality Assurance Laboratory

Project Management
Risk Management
Peer Reviews
Implementation of IV&V
Conduct Management System and Compliance Audits
Monitor and Assess overall Program and Project formulation and implementation process
Provide independent reviews/assessments of program/project performance, schedule and cost
Report BPR Items for Institutions and Programs

Oversight of Programmatic Resources (staffing, funds, training, information technology)
Effectively manage expenditure/investment decisions
Handling & Disposal of Hazardous, Contaminated & Controlled Substances

4.2 Financial Examples

Entity-level
Fund Balance with Treasury Management

- Treasury Information Maintenance
- Payment Confirmation Process
- Reconciliation and Reporting

Financial Reporting

- General Ledger (GL) Management
- Management Estimates
- Journal Voucher Processing
- Treasury Reporting
- Financial Statement and PAR Preparation
- Period End Processing

Budget Management

- Budget Formulation
- Budget Execution / Funds Distribution

Property Management

- *Personal Property*
  - Planning
  - Acquisition
    - *Purchase*
    - *Work In Progress (WIP)*
  - Managing and Accounting for Property
- *Operating Materials & Supplies*
  - Planning
  - Acquisition
  - Physical Inventory
- *Real Property*
  - Planning
  - Acquisition
    - *Purchase*
    - *WIP*
  - Managing and Accounting for Property
- *Contractor-Held*
  - Planning
  - Acquisition
    - *Purchase*
    - *WIP*
  - Managing and Accounting for Property
  - Physical Inventory
  - Managing and Accounting for Materials
- *Theme Assets*
  - Planning
  - Acquisition
    - *Purchase*
    - *WIP*
  - Managing and Accounting for Property
- *Internal Use Software*
  - Planning
  - Acquisition
    - *Purchase*

- - - *WIP*
    - Managing and Accounting for Property
  - *Capital Leases*
    - Planning
    - Acquisition
    - Managing and Accounting for Property

Grants Management

- Application
- Award
- Drawdown
- Monitoring
- Closeout

Procurement and Payment Management

- Purchasing
- Receipt of Goods
- Recording of the Liability for Services Contracts
- Invoice Validation
- Disbursements
- Vendor Maintenance
- Contract Closeout
- IPAC Processing
- Travel Processing
- International Payments
- Government Issued Credit Cards
- Review of Unliquidated Balances
- Reimbursable Agreements
- Payments for NASA working capital funds

Revenue and Receivables Management

- Intra-governmental Reimbursable Agreements
- Non-Federal Reimbursable Agreements
- Customer File Maintenance
- Other Receivables

HR and Payroll Management

- Personnel and Payroll Master File Maintenance
- Time and Attendance (Webtads)
- Automated Labor Distribution System (ALDS)
- Payroll Processing
- Reporting and Monitoring
- Pension/Post-Retirement/Other Benefits

Investment Management

- Acquisition
- Investment Management
- Interest
- Disposal

Information Technology

Cost Management

- Monthly Cost Assessments
- Working Capital Fund

4.3 Institutional Examples

OCIO

- Information and Information Technology Management
- Information Technology Security and Privacy
- IT Strategic Plans
- Enterprise Architecture
- IT Capital Investment
- IT Technical and Architecture Standards
- Records Management
- Integrated Enterprise Management Program (IEMP)

OCHMO

- Occupational Health Oversight
- Oversight of Aerospace Medicine Programs Areas

OGC

- General Law
- Space Act Agreements
- Export/Import Control
- Contracts & Procurement Law
- Partnering with Commercial Organizations
- Commercialization of NASA Activities
- Intellectual Property Law
- International Law
- Ethics Program

Office of External Relations

- Coordination of International, Cooperative, Reimbursable, & Partnership Activities
- Facilitation in implementing international programs/projects in each Mission Directorate
- Interactions with Executive Branch Departments & Agencies
- Principal Agency Representative with National Security Council, Office of Science & Technology Policy, State Dept, & DOD
- Support for Federal Advisory Committees and interagency activities
- Promotion of NASA history, both past and current achievements and activities

STRATEGIC COMMUNICATIONS
Education

- Strategic Education Investments
- Liaison with Higher Education Organizations
- Liaison with Elementary & Secondary Education Organizations
- Opportunities for Informal Education Support
- Education Technology & Products
- Educational Interactions with Flight Projects
- Minority University Research and Education Program (MUREP)

Legislative

- Legislative Support for Annual NASA Budget & Appropriations
- Legislative Support for NASA Authorization
- Liaison with Legislative Representatives at Field Centers
- Mission & Mission Support Liaison for Legislative Activities

Public Affairs

- Internal News & Communications
- NASA Press Office Management
- HQ Liaison for Public Affairs
- Multimedia Support for Public Affairs
- Art, Entertainment, Documentary Activities of Public Affairs Office
- Internet Services for Externally Published News and Communications
- Public Outreach Program
- Public Communications & Inquiries (FOIA)
- Management of Astronaut Appearances & Speakers Bureau
- Reporting on Television, Still Photo, & Public Inquiries Contracts

OIPP (Office of Innovative Partnerships Program)

- International Agreements
- Technical Development Partnerships
- SBIR/STTR Program
- Investment Seed Funding
- Centennial Challenges Program
- Innovative Partnerships
- FAST Program
- Innovation Transfusion Program
- Licensing of NASA Technology
- Intellectual Property Management
- Cooperative Agreements
- Protection of NASA Technology in coordination with the Office of External Relations

OFFICE OF INSTITUTIONS AND MANAGEMENT

Office of Internal Controls & Management Systems (OICMS)

- Directives Mgt
- OIG/GAO Liaison & Audit Follow-up
- Internal Control Program Management

Office of Infrastructure & Administration

Aircraft

- Mission Management Aircraft
- Aviation Safety
- Aircraft Operations

Environmental

- Environmental Restoration
- Environmental Management Systems
- Programmatic Environmental Coordination
- Environmental Laws Compliance
- Energy Management

Facilities

- Maintenance of Facilities & Real Property
- Planning & Real Estate Management

Logistics

- Integrated Asset Management
- Transportation and Travel Mgt
- Contract Property Mgt
- Property Disposal Mgt
- Industry Relations
- Equipment Mgt
- Materials and Inventory Mgt

ODEO

- EEO Complaints Processing
- ADR Program
- EEO/EO Grants Related Program

Office of Procurement

- Acquisition Planning
- Award of Contracts, Grants, & Other Procurement Instruments
- Contract/Grant Management & Administration
- Contract Closeout

OSPP

- Emergency Preparedness Planning
- DHS R&D Coordination
- Information Assurance
- Personnel Security & Asset Protection
- Safeguards and Program Protection
- Administrative Oversight of Agency-wide Security and Program Protection Organizations

OHCM

- Workforce Planning and Alignment
- Leadership Development
- Performance Management
- Talent Management
- Human Capital Accountability System

NASA Shared Services Center (NSSC)

- Business and Administration
- Implementation of NASA Services
- Accessibility of Services
- Quality of Services
- Service Delivery
- Customer Satisfaction and Communication
- Grants Management

Small Business Programs

- SBP in Support of Exploration and Space Operations Systems
- SBP in Support of Aeronautics Research
- SBP in Support of Science

Budget Management and Systems Support

- Budget Formulation
- Budget Execution
- Accounting and Processing
- Travel Program
- Business Systems User Access and Account Security

Headquarters Operations

- HQ Equal Opportunity and Diversity Management
- HQ Information Technology & Communications
- HQ Facilities and Administrative Services
- HQ Human Resources